2010

Analiza ruchu w sieci

przy pomocy programu Wireshark

[Wpisz tutaj streszczenie dokumentu. Streszczenie jest zazwyczaj krótkim podsumowaniem treści dokumentu. Wpisz tutaj streszczenie dokumentu. Streszczenie jest zazwyczaj krótkim podsumowaniem treści dokumentu.]

> Konrad Fierek Podstawy audytu sieci komputerowych 2010-06-01



1. Pierwsze uruchomienie - rozpoczęcie

Skanowanie całego ruchu sieciowego



Po uruchomieniu programu wita nas okienko powitalne.

Interesujące nas opcje znajdują się w grupie CAPTURE.

Aby rozpocząć przechwytywanie pakietów, wybieramy z "Interface List" interfejs sieciowy, przy pomocy którego chcemy przechwytywać pakiety.

	• Epres	ion One Apply		
Nu. Tone 1 6.000000 0.13107 1 1.251457 1.251457 1 1.251457 1.35177 1 1.251457 1.35170 1 0.00000 7.1.09133 1 0.00000 7.1.09133 1 0.00000 7.1.09133 1 0.00000 7.1.09133 1 0.00000 1.00000 1 1.33170 1.1.33170 1 4.350200 1.35170 1 4.350200 1.35255 1 5.33235 1.7.033234 1 4.352500 1.0.275966 Frame 1511200 (A2 bytes 5thermet 11, Stric Cisco Address Resolution Frod 1.97516	Source Fe801 (#980) 9851 (0713) acces Quarta ct., 05: 35: Fe 10.7, 12.18 Fe801: 4525: cs401 Goal, fcc3 Quart ac., 05: 35: Fe Fe801: 4525: cs401 Goal, fcc3 Quart ac., 05: 35: Fe Fe801: 4525: cs401 Goal, fcc3 Te801: 4525: cs401 Goal, fcc3 T	Definition Ff0211c Broadcast 210,255,255,250 Ff0211c Broadcast Ff0211c Broadcast Ff0211c Broadcast Ff0211c Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast	Pintoci SOP SAP SOP SOP AP SOP AP SOP AP SOP AP SOP AP SOP AP SOP AP SOP AP SOP AP SOP SOP SOP SOP SOP SOP SOP SO	Inte N=SEARCH * NTTP/1.1 who has 10.7.1.87 N=SEARCH * NTTP/1.1 N=SEARCH * NTTP/1.1 N=SEARCH * NTTP/1.1 N=Do has 10.7.1.87 N=Do has 10.7.1.87 ToTI 10.7.12.20 N=SEARCH * NTTP/1.1 N=SEARCH * NTTP/1.2 N=SEARCH * NTTP/1.3 N=SEARCH * NTEN SEARCH * NTH * NO.7.1.2.30 N=SEARCH * NTH * NO.7.1.87 N=SEARCH * NTH

2. Opis podstawowego okna programu

1	And the second	Definion	de,filtuscji w	yświetlania	
Time	Searce	D	rution	Protocol Info	
					(Sand)
Okno	z listą przechwyconych	pakietów			
Zawartość zazn	aczonego pakietu				
Zawartość zazn	aczonego pakietu				
Zawartość zazn	aczonego pakietu				
Zawartość zazn	aczonego pakietu				
Zawartość zazn	aczonego pakietu				
Zawartość zazn	aczonego pakietu				
Zawartość zazn swartość RAW z	aczonego pakietu aznaczonego pakietu				

3. Skanowanie ruchu pochodzącego z konkretnego komputera

Po włączeniu przechwytywania pakietów widzimy, jak wielka ilość informacji jest przez naszą sieć transmitowana.

Beates, STUELSBC(F)/0111C(F) Famil	y PC-E GIE NIC Centuring - Wintsham	and the second se	And in case of the local division of the loc	
Bie ficht Dies fin Capture ftr	udyze Statistics Telephony Isole Help			
如此变更更是 正司	X25 4+471	DDD BE	E 4 0	5 % H
Fjilter:	• types	on One Apply		
fin. Time	Soane	Destination	Perfocal	Into
1 0.000000 2 0.135197 3 1.262147 4 1.581574	fe80:1e968:9a8f:67f3ia6c8 QuantaCn_0c:35:fe 10.7,12.18 fe80:16525:ca40:6ca1:fcc3 puertece or 15:fe	ff0211c Broadcast 210.255.255.250 ff0211c Broadcast	550P ARP 550P 550P	<pre># SEARCH = HTTP/1.1 sho has 10.7.1.2.7 Tell 10.7.12.30 # SEARCH = HTTP/1.1 # SEARCH = HTTP/1.1 # SEARCH = HTTP/1.1</pre>
7 1.698153 8 1.698465	222	XXX	X	
10 2.000011 11 3.135170 12 4.381570 13 4.035158 14 5.939293	fellorresob;sast:off1:sdc8 Quantato_0c:35:fe fellor:6525:ca40;6ca1:fcc3 Quantato_0c:35:fe fellor:5cfd13d20;4a0a:se3e	Froadcast ff02::e Broadcast ff02::112	ARP SSDP ARP DHCPV6	M-basen - m10/11 Mo bas 10.7.1.87 Tell 10.7.12.30 M-58460M * HTTP/11 Who has 10.7.1.87 Tell 10.7.12.30 Solidit
15 5,999196 16 6,135255 17 7,635214 11 17 55354 19 4,275566	fe80::e90::54a8f:87f3;a6c8 Quantaco_0c:35:fe Quantaco_0c:35:fe Douartaco_0c:35:fe	FF02::e Broadcast Broadcast Broadcast	SSDP ARP ARP	H - SEAK H * WTH/1.1 who has 10.7.1.87 Tell 10.7.12.30 who has 10.7.1.87 Tell 10.7.12.30 Metho Stars EVAL ACCESSION AND ADDRESS IN THE SEARCH AND ADDRESS Method Stars EVAL ACCESSION AND ADDRESS IN THE SEARCH AND ADDRESS Method Stars EVAL ADDRESS IN THE ADDRESS IN THE SEARCH AND ADDRESS Method Stars EVAL ADDRESS IN THE ADDRESS IN THE SEARCH AND ADDRESS INTO ADDR
= Ethernet II, Src: Cisco = Address Resolution Proto	fe:00:4e (00:dd:ff:f0:00:4e), Dst: col (request)	Broadcast (ff:ff:ff		
0000 ff ff fr fr fr fr c0 0010 08 00 06 04 00 01 06 0020 08 00 00 00 00 00 00	d0 ff f9 00 4e 08 06 00 01 d0 ff f9 00 4e 0a 07 0c 16	· · · · · · · · · · · · · · · · · · ·		
Realist WILLIGS (P)/BILL(P) Famil	y PCI-F Factors 135509 Digitaryasi 155611 Marka	¢.0		Profile Default

Całą moc pakiet Wireshark ma w tzw. filtrach, które pozwalają zawęzić znacząco wyniki poszukiwań wg ustalonych kryteriów.

Na początku postaramy zawęzić kryteria poszukiwania, aby znajdować pakiety skierowane tylko od/do określonego komputera.

Jeśli zależy nam na tym, alby filtrować komputer po adresie IP, w pole filtru wpisujemy:

ip.addr == 1.2.3.4

gdzie 1.2.3.4 to adres IP, wg którego chcemy filtrować.

Fither: gr.addr c c 212.101.89.80	•	Egonation_ Clear Apply		
No., Time	Source	Destination	Protocol	Info
TERTING THEY ADDREST	100 Mar 10 Mar	COLUMN STATES	100	
158110 2202 6004 J	211 191 49 40	10 7 12 72	TCR	here a 37366 SVM ark) Second Arkal Minustata Lenie MCCalded WS
1551200 22002 5650514	1012512322	0100101039160	TON	AVARA INTO (451) sent singl rend
158120 2202 660514	1002012022	212 101 89,160	TOP	17566 - http://8511.540-1 wined Lwn-0
158121 2202.661548	212,191,89,60	10.7.12.22	TCP	[TCP segment of a reassembled PON]
158121 2202.661548	212.191.89.60	10.7.12.22	TCP	[TCP segment of a reassembled rou]
158122 2202.881552	212.191.60.60	10.7.12.22	TCP	[TCP segment of a reassembled FOU]
158122 2202.001552	212,191,89,60	10.7.12.22	TCP.	[TCP segment of a reassembled POU]
158123 2202.801554	212.191.89.90	10,7,12,22	HTTP	HTTP/1,1 200 OK (LENE/HEAL)
158123 2202.001554	252,191,89,60	10.7.12.22	HITP	HTTP/L1 200 CR (TRIT/PERF)
158124 2202 661557	212 197 89 68	10.7.12.22	100	here a \$7565 EVA are seen area almentates i pred attactant at
155125 2202 881559	217,147,89,60	10.7.12.22	TER	http: > 57567 [Syn. ACK] Sede0 Ackel win-65515 Lene0 #05-1460 as
58125 2202 661559	212,191,89,60	10.7.12.22	TEP	http > 57567 [svn, Ack] sege0 Ack-1 win-65535 t.en=0 NSt-1460 ws
55126 2202 561621	10.7712822	212.191.39.60	TCP	57565 > http (RST) Seg-1 win-0 Len-0
158176 2202 661628	10.7.12.22	212.191.89.60	TCP	57565 > http [RST] Segal winad Lenad
ESH17/22007/ESH518	100201-020	117,101,39,60	1204	TARK - NOR ACKI SHOWI AREALA WITHINGO LOTED
AT DRIVEN SOLD BOTTALS	COVER FIRST			17588 - mita (ACK) Sep-778 Atks/218 ath-84/00 Lan-0
Ethernet II, Src: Ibs_d5:	c7:16 (00:0d:60:d5:c7:16). 6	st: Cisco_f9:00:4e (00:6	0:11:19:00:4	e)
Internet Protocol, Src: J Transmission Control Prot Source port: http: (60) Sequence number: 27564 [Stream index: 279] Sequence number: 1 [Vext sequence number: acknowledgement number: usader Janeth. 20 betw	12.101 80 00 (212.101 80.00) acol, Src Port: http:(80), 1 (37584) relative sequence number) 1451 (relative sequence 1 773 (relative ack number	, Ont: 10.7.12,22 (10.7. NE Port: 57564 (57564), NeEPort: 10.1564 (57564),	12.22) Seq: 1, Ack;	773, sen: 1460
Imment Pratocol, Frici 2 Transmission Control Prot Source port: http (60) Destination port: 57566 [Stram index: 220] Sequence number: 1 (Jevet Sequence number: acknowledgement number: Hander Tength: 20 bytem - the set of Frank	12.101,50.00 (212.101,80.00) acol, Src Port: http:(80), 1 (37364) relative sequence number) 1461 (relative sequence 1 773 (relative ack number	, Oot: 10.7.12.22 (10.7. NE Port: 57384 (57584), NeEber)]	12.22) Seq: 1, Ack;	773, sen: 1460
Immerner Pratocol, Grc: 2 Transmitskom control Prot Source port: http (60) Destination port: 57566 [Stram index: 233] Sequence number: 1 (Next Sequence number: Acknowledgement number: Acknowledgement number: Nauder Ength: 20 bytm 0 0 00 d0 07 ff 93 00 44 00 0 0 0 c6 00 50 e0 dc b1 30 80 52 58 es 00 00 48 30 30 30 20 47 db 00 0 50 22 c0 30 39 20 48 75 0 28 48 30 20 20 47	12.101 80 00 (212.101 80 00) acol, src Port: http:(40), 1 (37544) relative sequence number) 1461 (relative sequence 1 773 (relative sequence 1 773 (relative sequence 1 773 (relative set number) 16 50 45 c7 16 36 00 45 00 16 50 12 44 0f 59 3c 0a 67 71 46 56 05 c7 13 50 10 44 55 3a 20 57 50 54 16 65 3a 20 57 56 54 16 70 62 30 31 00 30 31 34 16 40 59 46 59 35 77 78	, Ont: 10.7.12.22 (10.7. st Part: 37364 (37564), weber)]) N	12,22) Seq: 1, Ack)	773, Leni 1460
Innernet Pratocol, Frc: 2 Transmission Control Prot Source port: http (80) Destination port: 57566 [Stram index: 229] Sequence number: 1 (Next sequence number: Hadrowledgement number: Hadr	12.101, 80, 80, 727, 191, 80, 80, acol, Src Port: http:(80), 1 (37344) relative sequence number) 1461 (relative sequence 1 773 (relative sequence 1 775 (relative sequen	. Ont: 10.7.12.22 (10.7. mat.port: 17364 (17564). 	12,22) Seq: 1, Ack)	773, ien: 1460

Jeśli zależy nam na odszukaniu hosta po adresie fizycznym MAC, to wpisujemy

eth.addr == 11:22:ff:ff:22:11

gdzie 11:22:ff:ff:22:11 to adres fizyczny karty sieciowej.

Film HPL	NAM 13-23-8/8223-15	• ia-	esian. Des Apply			
Ne - 158918 158021 158921 158924 158924	Tere 1933, 234835 2322, 555973 2333, 234945 2333, 234945 2331, 234945	30000 C1500_79100140 C1500_79100140 C1500_79100140 C1500_79100140 C1500_79100140	Destruction Broadcast Broadcast Broadcast Broadcast Broadcast	Premocel all all all all all all all all	bit min Rad 10.7.1.87 rel1 10.7.1.22 who Rad 10.7.1.87 rel1 10.7.12.22	
154050 154430	2114, 237003 1314, 237003	CREATED AND	Brookat	-9960 -10 -10 -10	A second ground with high characteristic second sec	
 Frame Sthurn Sthurn Dest Soar Type Transe 	130023 (30 bytes in wire at 11, Src: Cisro.f9100) instico: Ibe.d8:C7:16 (3 re: Cisro.f9:00:44 (30.4 : 19 (0x0000) at Sricost, Src: 10.7.1 issian Control Fratecol.	 59 Sytem captored) 48 (35 - 95 - 75 - 75 - 95 - 95 - 95 - 95 - 9	s) Ibw.d3:c7(10 (00)00 Det Port) fig (II), Se	2007 2007 11 E E E E E A A A A	16) 1129, Leni 3	
Sour Dest Sequ	ce port: 57504 (57504) instien port: ftp (21) sam index: 156] ence number: ILB (re)	ative sequence number)	155			
0000 00 0010 00 0020 13 0030 1e	04 60 d5 c7 16 09 d0 f 24 0a fb 40 80 80 60 0 f7 e0 a0 00 15 fa 3a 6 f4 bd 8c 00 80 50 57 4	f f9 00 4e 08 00 49 00 0 00 0a 07 0c 16 c3 58 d e0 4a 80 11 96 50 18 3; 4 00 0a 67 0c 16 c3 58				
a Tantuk F	TURING PORTING POLICE	Faciliatio 25000 Displayed 152004 Mi	erka±0		Welfac Defeed	

Jeśli szukamy kilku komputerów, możemy posłużyć się spójnikiem or

eth.addr == 11:22:ff:ff:22:11 or eth.addr == 11:33:ff:ff:33:11

Aby zastosować wykluczenie – czyli wszystkie adresy poza określonym, dodajemy z przodu wykrzyknik:

1000	!(ip.addr == 1.2.3.4)	i
i	!(eth.addr == 11:22:ff:ff:22:11)	į

4. Skanowanie konkretnego ruchu

Umiemy już podglądać ruch pochodzący od konkretnego hosta w naszej sieci. Jednak, jak widzimy, ilość rejestrowanych pakietów jest bardzo duża, a co za tym idzie, ich ręczna analiza bardzo czasochłonna i męcząca.

W tym rozdziale zaprezentowane zostaną dodatkowe filtry programu, umożliwiające wyselekcjonowanie nie tylko ruchu na poziomie konkretnego hosta, ale także konkretnego portu, a także nawet pakietów danych konkretnych usług sieciowych.

1) Sesje WWW

Na początek zajmiemy się podejrzeniem tego, jakie strony internetowe są pobierane przez nasz komputer. Gdy spojrzymy do teoretycznej dokumentacji protokołu HTTP wykorzystywanego do transmisji stron internetowych, zauważymy szybko, że działa on na porcie TCP/80. Wyfiltrujmy więc wszelakie pakiety napływające na ten port.

ile Edit Ties Go Cepture &	ulyze Statutics Telephony Isole He	4	FT 64 10		
iker; top.govt.v=80		Egnession. One Apply			
IL - Time	Source	Destination	Partocal	inta	
706 370. 6405NA	204.45.124.114	44677,544722	NOT P	HTTP/1-1 200 GK [feat/toxescrat]	
AND RUNSPACE	0.07/15/02/0	2010/05/02/04 010	HUTF	GET / complete/dearch761-p18cliterr=hadeup1ds=17259//4899/2401	1.75
/13 120.956238	200.85.129.139	10.7.12.22	HTTP	HTTP/I.1 200 OK (CART/Javasor fit)	
TALE PARTENCO	Langer Barran	TOTALER REPORT	10102		- 23
10 121.424500	209.85.129.159	10.7.12.22 RCON 008408 810	HITP	MUST AND AN (LEAT,) WAS IN THE DECIMAL AND A DECIMAL AND	
CORPORTED IN COM	07005702	STORES STORES		The West of Company of Company of Company of Company	.,25
24 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	209.83.129.139	STORE STORE STORE	1010	1/10/21 200 dk (Cext/)avasoript)	
22 10 10 20 10 20 10 20 10 10 10 10 10 10 10 10 10 10 10 10 10	107/41979	20041511001010	BITTE	Charles and the second s	1.25
725 122.20408L	209.83.129.139	10.7.12.22	HETP	HTTP/1.1 200 OK (text/javascript)	
7 83 1227 482992	103-0190-220	200.85,129,139	HITTH	ctate /compliance/searchap1-p14c11ent-approxp1ds-12210,5469992481	- 25
734 122-514271	309.83.179.139		HTTP	HTTP/1.1 200 OK (TEXT/14VANCPTDE)	-
736 122, 668048	209.85.129.139	10.7.12.22	HTTP	HTTP/1.1 200 OK (text/javascript)	
715 122 640881	10.7712.12	209.85.129.139	HITP	17102 > http://ackj.Seq=6942_ack=4822_wite=05710_tem=0 GET_/combilete/search751=018c11ent=Noteewards=17210_c4699_14891	125
741 122,980593	209.85,129.139	10.7.12.22	HTTP	HTTP/1.1 200 OK (text/javascript)	_
244 133 136801	309-45-139-139	10.7.17.22	HTTP	HTTP/L1 200 DV (Text/LavasryInt)	23
thernet II, src: Ibe di Internet II, src: Ibe di Internet Protocol, src: Transeission control Pro Hypertext Transfer Proto Line-based text data: to	<pre>inclus(00)001001001051c71165, t 209.85.129.139 (209.85.129.13 tocol, src Part: http (80), t col xt/javascript</pre>	st: C1sco_f9:00:4# (00:0 9), ost: 10.7.12.22 (10. st Port: 57102 (57102),	0:ff:f9:00: 7,12,22) 569: 2385,	4e) Ack: 4748, Len: 445	

Ukazuje się naszym oczom cały ruch sieciowy na porcie TCP/80. W chwili obecnej łatwiej już nam jest podejrzeć kod źródłowy pobieranych stron. Jednak wśród widocznych pakietów, znajduje się jeszcze sporo pakietów kontrolnych samego połączenia, z naszego punktu widzenia w chwili obecnej zupełnie nieprzydatnych, a tylko zaciemniających użyteczne dla nas dane.

Wykorzystajmy więc dedykowany filtr do analizy protokołu http

TO MANDEMAKE
49.000 TO 19.
CONCERNMENT OF A STATE
AND \$488 1944
99.4483
CONTRACTOR OF A

Teraz możemy przystąpić do głębszej analizy. Na czarnym tle widoczne są pakiety, zawierające żądania naszego klienta. Na zielonym zaś – odpowiedzi od docelowego serwera. Bezproblemowo obserwujemy wysłane przez nas nagłówki HTTP (rys. 3), jak i też otrzymane od serwera docelowego nagłówki i właściwą treść witryny (rys. 4).

Realized Of LILLOROPY, BLLLC (P) Family FG-6	GEE NIC: Capturing - Wintshall				B million
Bie Edit Diese Go Capture Analyze	Statistics Telephony Icole Help		101111111111111111	10211 at	
·····································			1 M 10	5 X II	
Fitter Mtp	• bg	ression Clene Apply			
No. True	Searce	Destination	Protecut	Infa	-
4557 743, 354527	194.0.251.202	10.7.12.22	STATE OF	HTTP/1.1 200 OK (JPEG JFIF Inage)	_
4601 743.475778 4611 743.481155	213.180.146.27	10,7,12,22 11,10,140,27	NTTP	HTTP/1.0 301 Roved Persanently (text/html)	
4642 743.732174 4648 743.740772	213.180.146.27 213.180.146.27	10.7.12.22 10.7.12.22 10.7.12.22	HTTP	HTTP/1.0 204 Not Modified HTTP/1.0 204 Not Modified HTTP/1.0 200 OK (Cext/Attal)	
4663 743,780879 4673 744,066870	213.180.146.27 213.180.191.381	10.7.12.22 10.7.12.22	HTTP	HTTP/1.0 200 0K (COCLCSS)	COLUMN STATE
4050 744.110219 74610/41055000	213.140.146.120	10.7.12.22 10.11.12.22	4TDs	013 /////dicaddi/com/1000/neture/in/100/neture/in/ HTTP/1.1 200 0K (application/s-(avascript) City/heterorynamysegneng com/0507000 milionreng/s22003200	
4717 744.570621	213.140.150.45	10.7.12.22	HITTH	HTTP/1.0 200 OK (application/s-javascript)	
<pre># Transelsion control Protocol # pypertext Transfer Protocol # GET / HTTP/1.1vin # [Expert Info (char/Sequer Request Wethol: GET Request Wethol: GET Request Wethol: HTTP/1.1 Accept: Image/ipeg, applica Accept-Language: pl-PL.Vin User-Agent: Mozifla/4.0 (cc Accept-Lencoding; gip, def] [truncated] cookie: onet_st Connection: Keep-Alive/vin Hogi: New.onet.pl/vin</pre>	<pre>i, Src Port: 57146 (37146), tce); GET / HTTP/1.1\r\n] tion/x-ms-application, images separtble; MSIE 8.0; window: late/r\n up_aci0=0000c9ms70300cs0c;</pre>	Dat Port: http (80); : pe/gif, application/xau : Wt 6.1: Trident/4.0; 20424161626364; onet_ub	eq: 1, Ack el+xe1, 1ma succ2; .ME	т 1, ten: 2122 pe/pjpeg, application/x-es-xbap, application/x-shockwave-f f сця 2.0.50727; .мет сця 3.5.30729; .мет сця 3.0.30729; м 2016239185010043; onetzuo_ticket-ba855337D5906с4#A6144#106	Tash, app edTa Cent 238613401



W chwili obecnej jesteśmy w stanie przechwycić wszystkie użyteczne pakiety WWW. Jednak czasami i to kryterium zwraca zbyt dużo wyników. Zawęźmy więc poszukiwania pakietów na te, które skierowane są do serwisu internetowego, który mamy pod lupą.

http.host == www.onet.pl

Ujrzymy na ekranie wszystkie żądania pobrań strony, skierowane do serwera www.onet.pl

2) Autoryzacja WWW

Teraz przystąpimy do trudniejszych spraw ⁽²⁾ - czyli szybkiej analizy ruchu HTTP pod kątem wprowadzanych danych autoryzacyjnych. Wyróżniamy zasadnicze dwa sposoby poświadczania swoich uprawnień – standardowy formularz HTML, wysyłający metodą POST dane autoryzacyjne, oraz autoryzacja przeglądarką - HTTP/Basic.

a) formularz logowania POST

Przykładowy formularz autoryzacyjny widzimy na rysunku poniżej.

-	Squi	rrelMail
G	0	webmail for- nuts
5q By th	uirrelMail versioe « SquirrelMail Pro	1.4.15 ject Team
5	iquirrelMail L	ogia
Name:		
Password		
	Login	

Aby podsłuchać dane, które nasz system wyśle po kliknięciu przycisku Login, ustawiamy następujący filtr:

Reates STUDIOSCOPPOLISCIPI Fam	ly FCI-E GEE NIC: Capturing - Winnham			(ACHE)
ble [dit]]een (]o [_epture å te su and on and in and	nelyze Statutics Telephony Ipole		0. 271 28 18	
	N SO C T T T		u, ⊡ # 0 6 4 12	
Filter: [(http://coll == neteary pl) and (Mtp.request.method ++ POST)	 Egression Clear Apply 	In succession of the second	
Illi - Time	Southe	Destinution	Pertocal Info	
Frame 11587 (024 bytes Ethernet II, Src: Cisco Enternet Protocol, Sri	on w(re, 924 bytes captured) _f0:00:44 (00:d0:ff:f0:00:44 10:11:27 [10:7 12:27] p) a), Dat: Ibe_d5:c7:16 (0 11: 62:29.101.105 (02.29	0-0d:60:d5:c7:10) 1401-147	
Frame 11587 (924 bytes Ethernet II, Src: cisco Enternet Protocol Srii Tranafision Control Pr Sypertext Transfar Prot	an wire, 924 bytes captured) _F9:00:44 (00:40:ff:f9:00:44 _90:7:12:27 (10:7:12:27), 99 atotal, Src Part: 57307 (57) atol) a), Dat: Ibm_d5;c7:16 (0 19: 62:20 11: 107 (NJ.20 207), Dat Port: http (80	0-0d:60:d5:c7:18) 1481-1871), 5eg: 1, Ack: 1, Len: 870	
Frame 11587 (924 Bytes Ethernet II, Src: Cisco Enternet Protocol, SrcI Transmission Control Pr Hypertext Transfer Prot Line-based text data: a hypercentration protocol	an wire, 924 bytes captured f9:00:44 (Colido:ff:f9:00:44 Do. 11.27 ff0:17.27), 99 docull, Sr. Fart: 57207 (17 acol aplication/x-www-form-orleon) e), Dat: The_d5:c7:16 (0 16 62:ca.101 10* (02.20 07), Dat Port: http (80 coded)permittable2.	0:0d:60:d5:c7:16) .141.1071), 5eq: 1, Ack: 3, Len: 870	
Frame 11387 (924 bytes Ethernet II, Src: Cisco Internet Protocol, Srd Transission Control Pr Dypertext Transfer Prot Line-based text data: a Notifice england intern	an wire, 924 bytes captured) f0:00:44 (00:00:1f:10:00:44 10:11.22 (00:11:22) o docul, Src Part: 57207 (372 acol plication/x-www-form-urlens)), Dst: The d5:c7:16 (0 16 - 22 - 16 - 20 - 64 - 20 17 - 75 - 20 - 16 - 20 10 - 20 - 20 coded)metoare110212 - artoderec	0:04:60:45:c7:10) 14111071), 543:1, Ack: 1, Len: 870	
Frame 11587 (924 bytes Ethernet II, Src: cisco Internet Protocol Srid Transfision Control Pr Sypertext Transfer Prot Line-based text data: a Tryth.corrector.	an wire, 024 bytes captured) f0:00:44 (00:00:ff:f0:00:44 00.7 11.22 (10:7 12:22) (00 docul, src Part: 57707 (57 acol aplication,x-www-Form-urlence aplication,x-www-Form-urlence) a), Dat: The_d5:c7:18 (0 HEI-62:20.011.107.987.20 207), Dat Port: Hotp (80 coded 	0-0d:60:d5:c7:18) 181:1871 } } Seg: 1, Ack: 1, Len: 870 	
Frame 11567 (024 bytes Ethernet II, Src: Cisco Internet Protocol, Srci Transmission Control - mypertext Transfer Prot Line-based text data: a Toyong control protocol	an wire, 934 bytes captured f0:00:44 (COLID: If:10:00:44 DO: 21.22 (I0:1 17.22) 9 docul, src Part: 57207 (S72 col) aplication/x-www-Form-orlenc while documents and the second) a), Dat: The_d5:c7:16 (0 10 c2.ca.10 inc.10 coded coded () minimized c2) = actoin to-	0:0d:60:d5:c7:10) /100:1073), Seg: 1, Ack: 1, Len: 870 ////////////////////////////////////	
Frame 11587 (924 Sytes Ethernet IT, Src: Cisco Internet Protocol, Srci Transistion Control Pr Hypertext Transfer Prot Line-based text data: a hypertext Transfer Prot Line-based text data: a	an wire, 924 bytes captured) f9:00:44 (30:10:1f:f9:00:44 tocul, Src fert: 57207 (17 acol aplication, x-wwe-form-orlans aplication, x-wwe-form-orlans acol) e), Dat: The_d5:c7:16 (0 11 02:20 101 100 (07.00 07), Dat Port: http (80 coded 1) minimize(c2) = minimize 0 /1412*37 8012/800	0:0d:60:d5:c7:18) .181.1873), 580:1, Ack: 1, Len: 870	
Frame 11587 (024 bytes Ethernet II, Src: cisco Enternet Protecol. Sful hypertext Transfer Brot Line-based text data: a Loginary and text data: a 1990 27 25 24 24 25 34 25 200 25 38 62 54 00 0a 00 200 27 25 24 24 25 34 25 200 27 25 25 200 27 25 200 200 200 200 200 2	an wire, 024 bytes captured) F0:00:44 (50:00:1f:19:00:44 00:11.27 (10:01:42) po atocul, Src Port: 57307 (573 acol plication,x-www-Form-urless plication,x-www-Form-urless 04 200 10 20 20 20 20 20 3 04 20 10 20 20 20 20 20 3 10 20 20 20 20 20 20 20 20 3 10 20 20 20 20 20 20 20 20 3 10 20 20 20 20 20 20 20 20 3 10 20 20 20 20 20 20 20 20 3 10 20 20 20 20 20 20 20 20 3 10 20 20 20 20 20 20 20 20 20 3 10 20 20 20 20 20 20 20 20 20 3 10 20 20 20 20 20 20 20 20 20 20 20 20 20	<pre>0</pre>	0:0d:60:d5:c7:18) 188118079 }, Seg: 1, Ack: 1, Len: 870 	
STO 37 24 34 34 54 34 37 STO 37 24 34 54 54 54 34 37 STO 37 24 34 54 54 54 34 37 STO 37 24 34 54 54 54 54 37 STO 37 24 34 54 54 54 54 54 37 STO 37 24 34 54 54 54 54 54 54 STO 37 24 34 54 54 54 54 54 54 STO 37 24 34 54 54 54 54 54 54 STO 37 24 34 54 54 54 54 54 54 54 STO 37 24 34 54 54 54 54 54 54 54 54 54 STO 37 24 54 54 54 54 54 54 54 54 54 54 54 54 54	an wife, 024 bytes captured f0:00:44 (Coido:ff:f0:00:44 Docul, Src Fort: 57207 (Sr2 acd) aplication/x-www.Form-orlers with 04 20 04 33 01 3 07 36 3 04 25 07 0 00 17 01 10 05 01 7 01 05 17 05 05 10 05 01 05 00 05 17 05 10 05 01 05 00 05 17 05 10 05 01 05 00 05 17 05 10 05 00 05 00 05 17 05 10 05 00 05 00 05 10 05 00 10 05 00 10 05 00 10 05 00 10 05 00 10 05 10 05) a), Dat: The_d5:c7:16 (0 10 G2:00 INL 107 (02.00 coded 0 /1412+39 Butaredo 0 /1412+39 Butaredo 0 eBod 100/1000 0 eBod 100/1000 0 eBod	0:0d:60:d5:c7:16) /100110079), Seq: 1, Ack: 1, Len: 870 ////////////////////////////////////	

Filtr zwróci nam wtedy wszystkie pakiety, które zawierają w sobie dane wysyłane do serwera metodą POST. Widzimy więc dokładnie podane przez użytkownika w formularzu dane autoryzacyjne, takie jak nazwa użytkownika i tajne hasło.

b) autoryzacja HTTP

Drugą z używanych powszechnie metod, jest tzw. autoryzacja HTTP. Po wejściu na chronioną stronę wita nas takie oto okienko przeglądarki:

?	Witryna http://www.fiercio.pl żąda podania nazwy użytkownika i hasła. Komunikat witryny: "Ograniczony dostep"
żytkownik:	jkowalski
Hasło:	*****

Aby wyfiltrować bezpośrednio dane, ustawiamy filtr

Image: Solution of the second seco	
Fiber (Nttp-host +-+ www.Hercio.pt) and (http-authonumion) - Egyression. Creg: Apply Na. Time Source Source Particular Info 12551 - 2222, 13,6048 - 015-12,223 - 02551 - 0255 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0110 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0100 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 -	
III. Time Boards Definition Perform Info	
17561-7421, 18608 1017-12,77 227-31-217 HTTP OCT /Setters HTTP/1.1	
HERT (Section) HTTP://///	
Host: www.fiercio.pl/r/n User-Agent: Mozilla/5.0 (windows; u; windows WT 6.1; p]; rv:1.8.2) Gecko/20100115 Firefox/J.6/r/n	

Widzimy nasz szukany pakiet. Zawiera on nagłówek Authorization i pewien ciąg znaków, będący frazą autoryzacyjną. Filtr Wiresharka pozwoli nam zdekodować tę frazę do czytelniejszej postaci. Aby zrobić to, klikamy po prostu na plusik przy Autorization. Pokażą nam się wtedy dane autoryzacyjne w postaci NazwaUżytkownika:Hasło.

Beats	a millialC(P)/0111C(P) Family PCI-8 GI	IE NIC: Capitoring - Wireshare	and the second second	And States	C (C) (C) (C) (C) (C) (C) (C) (C) (C) (C
Bie Be	it Time Go Capture Analyze 30	atutics Telephony Lools Help			
		A + + + + + 2	E B Q Q C		
Filter: 0	http://est == www.fiercio.pl) and (http:a-	rthorization) • Eg	ression One Apply		
No	Time	Source	Dectination	Partocal Info	-
17.58	CHEROLOGY AND	100000000000000000000000000000000000000		HTTP: GLT /SECURE HTTP/L.E	
H GE	T Jacuraj HTTP/1.1\r/s				
H0 U3 AC AC AC AC E E CO [T	st: www.fiertio.pl/r/n er-Agent: Mozilla/5.0 (win ccept text/hm),agelicatio ccept-Language: pl.en-us:qu/ ccept-Language: pl.en-us:qu/ ccept-chares: 150-6859-2.u sep-Alive: 115/r/n winection: keep-alive/r/n runcated] Cookle: comment_ thorization: Basic astvd2f	dows; U; Windows WT 6.1; ; n/xhtml+xml,applitation/xm 0.7;en;q=0.3)r\n e\r\n f=8;q=0.7;*;q=0.7\r\n author_8ac07002e74df44c04c ac2tpok#svulhs290vq==\r\n	i]; rv:1.9.2) Gecko/ i];q=0.9.*/*;q=0.8\r' 19e1518b50f738⊷¢x×v	0100115 Firefox/3.6\r\n n 1: :::::::::::::::::::::::::::::::::	the scitter of sciences, controls
1.0	An and a set of the se				

To tylko częściowy opis filtra HTTP.

Więcej informacji pod adresem: <u>http://www.wireshark.org/docs/dfref/h/http.html</u>

3) Sesje Gadu-Gadu

Gadu-Gadu to jeden z najpopularniejszych komunikatorów w Polsce. Dzięki Panu Arturowi Kołodziejowi możemy ściągnąć wtyczkę do Wiresharka, umożliwiającą analizę protokołu GG.

Opis instalacji oraz plik z wtyczką można znaleźć na stronie http://www.wireshark-gg.xt.pl/

Po skopiowaniu pliku GG.dll do katalogu plugins/ restartujemy Wiresharka.

Do okna filtrów wpisujemy

gg

a następnie obserwujemy pakiety z żądaniami logowania, wysyłanymi wiadomościami, a także zmianami statusów.

in lage	wanie gg.pcap	Wireshark					. 08
the t	de yew so s	apture Analyze Statistics	Fielb	-			
		E B X 2 B	4 4 4 4 7 2 1	. Q. Q	9, 🖻 🖉 🗖	8 % 32	
Elter:			▼ Expres	sion Glear As	anky .		
No	Tate 1 0.000000 2 0.016998 3 0.017086 4 0.031762 5 0.03278 6 0.051717	Source 192,168,16,72 91,197,13,14 192,168,16,72 91,197,13,14 192,165,16,72 91,197,13,14	Destination 91, 197, 15, 14 192, 168, 16, 72 91, 197, 13, 14 192, 168, 16, 72 9109 (27, 13) 44 192, 168, 16, 72	Protocol TCP TCP GG GG TCP	Info Tpitp = https https = fpitp fpitp > https Typ Pakieturit https > foitp	[SYN] Seq-U wine16584 Len=0 MSS-1 [SYN, ACK] Seyed Ackel wine3840 L [ACK] Seq-1 Ackel wine17520 Len-D (22ba do wyznaczenia hashu hasla] opówania) [ACK] Seg-13 Ackel52 wine6432 Len	460 en=0
	Insmission co tokol os tokol os pp Pakietu: Plugosc pakie R GG: Skrot Hasla: Heznany: 162 Heznany: 259 (pp Opisu: Do Heznany: 238 Heznany: 259 (pp Opisu: Do Heznany: 259 (pp Opisu: Do Heznany: 268 (P: 0.0.0.0 (taxymalny roz Heznany: 190 (p): Lato, 1	ntrol Protocol, Src Logowanie (25) tu: 143 2 6680492 (0x60F52cac 844807 (0x2130c707) 931540 (0x86f518 847490 (0x86f518 847490 (0x86f5188 stepny (z opisem) (a: gg 7.7 (build 33 0x00000002) 84 (0x00004000) 6.72 (192.168.16.72 0.0.0.0) miar obrazka: 255 (0x00000be) ato ws2\352dzie zwa	<pre>Port: fpitp (1045), Ds)) 4) 15) (42)) r1owa\2630 pszala\2630</pre>	noje serce)	ps (443), Seq: 1,	Ack: 13, Len: 151	
0030 0040 0050 0060 0070	44 64 18 94 76 00 02 42 10 76 8d 88 00 00 00 00 00 00 00 00	00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<	ar 00 00 00 00 00 17 00 21 14 95 6b 04 22 v 00 00 00 00 00 00 00 00 00 00 00 00 00	···+			

EEE 802.11g Wireless Cord. 1	(Microsoft's Packet Scheduler) : Capturia	g Wireshark	
Elle Edit Yow Go Capture Ana	dyze Statistics Help		
現实更更更 正 团 :	お田田 ビタッカムギギ	■■■ Q Q Q E ■ M S S S B	
Oter: [gg	• E	ipression Qew Apply	
No. Tese Source 20 09.969087 01.19 31 013.345008 01.20 33 117.097868 01.20 34 117.097869 91.19 34 101.0097869 91.19 35 137.097869 91.20 36 139.63225 91.20 38 147.042933 01.20 40 144.225999 91.29 41 214.994666 91.59 42 166.009105 91.19 43 174.934666 91.59 44 174.934666 91.59 45 175.117874 91.19 91 1100000000000000000000000000000000000	Destruison 7, 13, 24 192, 168, 16, 71 7, 13, 24 192, 168, 16, 71 7, 13, 24 192, 168, 16, 71 7, 13, 24 192, 168, 16, 71 7, 13, 24 192, 168, 16, 71 7, 13, 24 192, 168, 16, 71 7, 13, 24 192, 168, 16, 71 7, 13, 24 192, 168, 16, 71 7, 13, 24 192, 168, 16, 71 7, 13, 24 192, 168, 16, 71 7, 13, 24 192, 168, 16, 71 7, 13, 24 192, 168, 16, 71 100, 168, 16, 71 00, 10, 168, 16, 71 100, 168, 16, 72 00, 10, 15, 00, 46, col 100 100, 163, 16, 72 192, 168, 16, 71 102, 168, 16, 72 192, 168, 16, 71 103, 24 192, 168, 16, 71 104, 164, 16, 72 192, 168, 16, 71 107, 164, 164, 72 192, 168, 16, 71 102, 168, 16, 72 192, 168, 16, 72 102, 168, 16, 72 192, 168, 16, 72 102, 168, 16, 72 192, 168, 16, 72 103, 50 101 mowy: 23890128 (0x016c88d0)	Potocol Info GG Typ Pakietu: [2mians Stanu] GG Typ Pakietu:	131, Len: 42
00000 00 00 22 96 72 44 0 0010 00 52 01 03 40 00 8 00200 01 18 08 04 11 84 7 00300 37 72 37 04 00 00 00 00 04 11 84 7 0440 00 00 00 00 04 12 14 00<00 00 00 04 04 88 62 01 2 00 0440 76 00 04 04 88 62 01 2 00 050 61 64 67 77 61 20 7	0 15 00 46 c4 c9 08 00 45 00 0 06 bf d6 c0 a8 10 47 5b c5 c 3d e0 44 41 59 ca b3 50 18 b 00 00 00 22 00 00 00 6b 17 8 00 00 00 70 72 7a 79 6b b3 7 59 61 64 6f 6d 6f 73 63 00		
were served to the second second difference of the	Restart Restarts #3 Destinant 24 Market ()	Dealling To	ala k

iEEE 802.11g Wirele	ss Gard. (Microsoft's Pac	ket Scheduler) : Captoring	Wiresbark		
Elle Edit yeaw Go Ca	pture Analyze Statistics (Bela			
SI M M M M M	图 X 22 目 (4 * * * 7 2 1		0, 22 🕷 12 🥵 🛸 13	
gter: gg		+ Dor	ession geer Ap	ay .	
No.+ True	Source	Destination	Protocol	Info	
20 56.189279	01.107.13.24	192.168.16.71	66	Typ Pakietu: [zelana Stanu]	
24 86 026604	01 307 12 34	1019101810171		TYPE FAM RECORD STORAGE STUDIES	
26 86,167999	91,197,13,24	192.168.16.71	65	Typ Pakietu: [2m]ana Stanu]	
27 86.177769	91,197,13,24	192,168,10,71	-06	Typ Pakietu: [2miana Stanu]	
29 89.969987	91.197.13.24	192,168,16,71	65	TVD Pakletu: Zmlana Stanul	
					S ()
Typ Pakietu: Niezmany: 18 NR 65: Typ Opisu: Do IP: 89.230.16 OCC Port: 1 Wersja Klient Maxymainy roz niezmany: 0 (2mlana stanu (23) (ox00000022) stepny (2) 1.240 (89.230.161.2) a: gg 7.6 (bulld 16) mlar obrazka: 100 ox00000000) 0x00000000)	40) 88) (41)			
0000 00 15 00 46 0010 00 42 32 af 0020 10 47 1f 8a 0030 19 20 bb 75	c4 c9 00 0e Ze 9b 40 00 3b 06 d3 3a 08 04 al 19 c9 47 00 00 17 00 00 00	7e 4a 08 00 45 00 . 5b c5 0d 18 c0 a8 . 7c 3d e0 4d 50 18 . 12 00 00 00 a6 6e .		. E.	
V040 B0 UD 02 79	60 81 LO 01 00 18	64 00 00 00 00 00 .	a Yaaa da	4.4.4	

4) Poczta elektroniczna – SMTP

Kolejnym naszym krokiem jest analiza listów elektronicznych wysyłanych przez nasz komputer. Możemy dzięki temu np. wyeliminować różnorakie programy wysyłające SPAM.

1	Por de autogrand - wienes			
on for Inn do Printin Su	while Traping I webside Tools Lieb		a maariya	
I S C S S S I I I	X C S I C P P O F			5 X 3
iter, sing	• 1	apression Oest Apply		
s. Time	Source	Destinution	Pertecut	inta
4264 686, 283972	195.88.50.50	10,7,12.22	SMTP	St 220 dpoczta.pl
4267 686, 310532	195.88.50.50	10.7.12.22	SMTP	5: 250-water, dhosting.pl 250-PiPELIMING 250-Size 52428800
4260 686 134233	195 \$8 50 50	102 00 10 20	MINT D	St. 334 VON COSTINUE
TENOR COMPLETING	102123 Eth 2 Aug	ACCREDINGUESO	1000	Concession and the second s
42/2 080, 15805/	195.68.50.30	10.7.11.22	SATE	S: 334 0GF2C3DVENUB
4274 846, 387638	195,88,50,50	10,7,12,22	SMTP	5: 235 2.7.0 Authentication successful
4277 686,417717	195.88.50.50	10.7.12.22	SMTP	5: 250 2.1.0 0k
4279 686, 433245	195.88.50.50	10.7.12.22	SMTP	St 250 2.1.5 ok
ADDI CALOR INDIANA	195 88 50 50	1010100000	COLUMN TWO IS NOT	REALAND ARE WITH ATRACES ATRACES
122400000000000	C.R.A.L.R.C.	10) 38,40,52	COLUMN TWO IS	CT ON A TRAZENT AND AVEC
4785 640 540416		105.88.30.50	5412	Trost exerciser effice outlook replequerta, plas, subjects effette str250-2.0.0 det duesed as 2406044400
		Concerned and the second	-	

W tym celu ustawiamy filtr

Widzimy całą historię komunikacji z serwerem pocztowym. Jednak, gdy wysyłanych wiadomości jest kilka równolegle, analiza poszczególnych kawałków może być trudna.

Jeśli chcemy wyfiltrować wstępnie tylko źródłowe adresy e-mail, z których wysyłane są wiadomości stosujemy filtr

Beats	a minimatic Pyrintic Pl Family PCI-E (IEE NIC: Capitaring - Wineshark		and the second		G (B #34
Bie Ba	it Ive Go Capture Analyze i	latistics Telephony Isole Help				
	· · · · · · · · · · · · · · · · · · ·	日々キキの女は		1 M M	1 🥦 斜 🛛 🖬	
Filter F	reg.command ++ "MAIL" and smip.ies	parameter contains "FROM" . Eg	pression Creat Apply			
No.	Time	Source	Destinution	Pertocil	Into	4
1.1.1	A TANKING SAN WALL	10000-1010-001	191- No. 50 50	SHIP	CT MADE # HERE HI IGHOOCZER. HTH	

Wyświetlą nam się wszystkie pakiety zawierające fazę MAIL FROM sesji SMTP.

Jeśli zaś interesują nas odbiorcy wiadomości, możemy ustawić filtr

mtp.req.com	nmand == "RCF	ר "די" די"			
Reates STUDIED/Fy0111C/F) Family F	CFE GBE NIC: Capturing - Winnshark	and the second second	-	himited	B
Sie Edit Time Go Capture Analy	en Statistics Telephony Isola Help				
	[김吕 < + + 7 호	BBQQQ!	1 🕷 🕅	8 ¥ B	
fillen (Mit Lington mand Law Sorth	• tpr	scon Clear Apply			
No. Tree	Source	Destinution	Protocal	Into	
1000 CON 100	STREET, STREET	195.86.50.50	1 BATTER	c appr to: -pledoucrta.pl>	

Jego rezultat to wyświetlenie wszystkich pakietów RCPT TO sesji SMTP.

4) Poczta elektroniczna - POP3

Drugą częścią analizy poczty jest analiza ruchu poczty odbieranej z naszego serwera pocztowego – serwera Post Office Protocol.

a) wiadomości

Na początek ustawmy filtr główny dla POP3

Realized, ITLEDOCOPYE	LLLC(P) Family PCI-E GBE NEC Capturing - Winterhalt		1.000	(LI)O	-
ie fat Den go	Gepture Analyze Statistics Telephony Icole He				
1 里 段 梁 章			四 條 10	5 ¥ H	
ter pop		Egpression Orag Apply			
time	Source	Destination	Protocol	İsta	_
95 8.490070	195, 88, 50, 50	10.7.12.22	POP	5: -ERR Invalid command.	_
100 8.501698	194.28.51.40	10.7.12.22	POP	S: +0K 0 D	
107 8,519023	195.88.50.50	10.7.12.22	POP	s: +ok Password required,	
117 8,543051	195.88,50.50	10.7.12.22	POP	S1 +0K Togged In.	-
110 5 56500	195 88 50 50	1033188580.500	POP	5: +0K # 158501	_
111111111111111111111111111111111111111		A REPORT OF A R	P CP	C Will	
119 8. 590080	195.88.50.30	10,7,12,22	404	S: +0K	
140 8 590209	10.0012.22	191.26, 51, 20	PCP		
148 8.613061	195.88.50.50	10.7.17.22	POP	s: +ok POP3 clients that break here, they violate stos3.	
153 8.621874	194,28,51,40	19,7,12,22	POP	8: +0# cogging out	
127 8 675472	105 88 50 50	10.2.13.22	1000	NI LOR 1247 OCTATE Follow	-
295 8.895945	195.88.50.50	10,7,12,22	POP	S: DATA fragment, 451 bytes	
424 314 72890	COMPANY AND ADDRESS	195.885.505.50	PGP	CONTRACTOR OF CONT	
430 9,513280	195.88.50.50	10.7.12.22	POP	ST HOK 6228 octets follow.	

Widzimy tu cały przebieg sesji z serwerem POP3.

Aby wyfiltrować jedynie wiadomości, wpisujemy jako filtr

рор	.respon and po	se.indicator p.response.d	== "+OK" escriptior	n con	tains "octets"	
a Realter	MTUBLOBC(Py0111C)P) Fan	ndy FCI-E GIE NIC: Cepturing - Winnheik		and the		C (0 (0 (0 (0 (0 (0 (0 (0 (0 (0 (0 (0 (0
DH 24	a a a a la lata	inelyze linguing and a set of the line line line line line line line lin		EI 😹 🗵	5 x 2	
Filter: In	tor " QK" and populatipo	nse description contains "octets follow"	Epression. One Apply			
5n., 17	Time 7 8,675472	195.88.50.50	10,7,12,22	Pop	bis Si +DK 1447 octets follow.	
46 50, 52, 53, 58, 58	8 9.623045 2 9.712769 2 9.806631 1 9.875073 0 9.955234 9 10.017938	195, 88, 50, 50 195, 88, 50, 50	10.7.12.22 10.7.12.22 10.7.12.22 10.7.12.22 10.7.12.22 10.7.12.22 10.7.12.22	POP POP POP POP POP POP	5: +0K 14443 acters follow. 5: +0K 4187 acters follow. 5: +0K 4379 acters follow. 5: +0K 15318 acters follow. 5: +0K 14227 acters follow. 5: +0K 14227 acters follow.	

Widzimy tu listę pakietów z pobieranymi przez klienta wiadomościami.

b) hasło

Jeśli zainteresowani jesteśmy przechwyceniem jawnego hasła, stosujemy

	pop.requ	est.command	== "PASS	5"		
Bastek	MTURDARC/Py/RELICIPI Family PCF-E	GBE NIC: Capituring - Wintshark		-		Child Bard
Bie Ede	è Dies Go Capture Analyze	Statistics Talaphony Isola Help				
8 H	N N N I N N N N	18 4 + + 6 72	EB QQQE		S 24 23	
Fites po	op request.command ++ "PASS"	• ige	ssion Oear Apply			
No.	Time	South	Destrution	Protocol	Infa	-
10	2	CONTRACTOR OF CONTRACTOR	A CONSTRAINT OF CONSTRAINT	100	Des 1955 Actionation	

Na liście zauważamy wszystkie podane przez nas hasła dostępowe w zupełnie jawnej postaci.

5) Przesył plików FTP

Ostatnim z analizowanych protokołów nie zakładających szyfrowania jest FTP. Służy on do zdalnego przesyłu plików. Zaobserwować możemy brak zabezpieczeń zarówno przesyłanych danych, jak i też nawet autoryzacji.

a) dane

Na wstępie przechwyćmy cały ruch FTP filtrem

111	antition(p)/ettic(P) Family PC-E OF	E NICi Capturing - Winnha	Statement of the local division in the local	1000	
Ein Ede	t Time Go Capture Analyze Sta	statics Telephony Icole	Help		
14 H	N N N I N N N N	品(ちゃゃの			5 2 2
fiter No	orftp-data		· Epression Clear Apply		
in .	Time	Source	Destination	Protocol	lefa
	844.1194443	and the state of the	144/7-14-22	FIR	Responses 200-
4287	844,742158	193.219.25.2	10.7.12.22	414	Response: 220- FTP na sunsite (6 TB oprogramowania).
4289	844,758075	101, 210, 25, 2	10.7.12.22	FTP	Response: III Guest login ok, send your complete e-mail address
4,000	TELEVISION ST	101 112 22	1931219128	FTU	Request PASS yoz Takexang a con
4291	844, \$06390	193.219.28.2	10,7,12,22	FTP	Response: 230-Please read the file README
4294	845.002090	193.219.28.2	10.7.12.22	3.15	Response: 230- it was last modified on the Jul 4 02:59:08 200.
4296	845.008582	193, 219, 28, 2	10,7,12,22	FTP	Response: 213 INIX Type: 18
920	AND CORROR	19:7.12.17	191,110,28	1 TP	Request Pro
4298	845,013861	193,219,25,7	10.7.12.22	FTP	Response: 257 "/" is current directory.
4100	845.019136	191,219,28,2	10.7.17.22	FTP	Response: 200 Type set to L
100	CONTRACTOR OF CONTRACTOR	100000000000000000000000000000000000000	TO PROTOTO A	ALC: N	NUMBER OF STREET, STREE
4302	845.036629	193, 219, 28, 2	10.7.12.22	#TP	Response: 227 Entering Passive Mode (193,219,28,2,225,66)
4 207	545 014015	100000000000000000000000000000000000000	101.210.211.2	2.7.11	Response: 550 // not a plain file
1000		100000000000000000000000000000000000000		Contract of the local division of the local	Responder as a number practice and a
4309	845.049879	193.219.25.2	10,7,12,22	#TP	Response: 550 /: not a plain file.

Widzimy dużo informacji odnośnie całej sesji – wstępne uwierzytelnienie, wyświetlanie listy plików w katalogach, historię zmian katalogów przez użytkownika, oraz same dane.

Jeśli interesują nas nazwy pobieranych plików, stosujemy

_	ftp.	req	uest	t.c	omr	na	nc	[=	=	"	RE	TR						
Realter	MURIAROPYRILLC)	P) Family FG	E GEE NIC. (Capituring	- Wintsh	ék –	-					-						E B B
Bie Edi	t Des Go Capt	in Anslyza	Statutics	Telepho	ny Iool	• H	elp:											
8 H	张敬荣 [1]	四米	2월	9.0	4.4	1	2	夏	8	Q.	q e	4.四	- 66	Ø	1 8 2	F [14	
Filter Th	proquest.command -	= "RETR"				•	Epre	ssion_	Gen	Appl								
No	Time		Sout	ix		_		Deri	inatio	in			Protoc	at .	Into			-
451	COLUMN STREET		10,					193	1.1.5	1.1			110		E. B. Garr	at a	NE311 /	

Prezentowane będą wtedy tylko pakiety z nakazem pobrania zasobów.

Jeśli zaś szukamy wysyłanych z naszej sieci plików, pomocny będzie filtr

	ftp.	requ	iest	.co	mm	an	d	==	"	ST	DR		-			
Realiza	autoresconvertici	7) Family PCI-L	GBE NIC. Cap Statution 7	muting - V	Vinishar	S.										0.0
			2 単一の	ζφ s	Loon	7 1	E //	65 (B)	e,	a a	£11		0 18	24	8	
Filter 1	prequest.command -	- '3108"				• 5	gressi	wi. Ce	e App	y						
No	Time		Source	1.17				Destruti				Pretocel	H	i i an	when puttone lots	-

b) hasło

Protokół FTP także nie szyfruje w żaden sposób hasła. Aby poznać pary login/hasło, stosujemy

Ftp	.request.c	ommand == "	USER" or	ftp	.request.command == "PASS"
a lautak	RTuB168C(P)/8111C(P) Family PCI-E G	BE NIC: Capituring - Wireshark			Ci (Ci (Ci (Ci (Ci (Ci (Ci (Ci (Ci (Ci (
Die Ede	Den Go Capture Analyze S	latistics Telephony Icole Help			
		B 4++072	BBQQQE		5 x 3
Fitter No.	request.command ++ "USER" or hput	equest.command "FASS" - Egree	sion Clear Apply		
No	Time	Source	Destination	Perfocal	inta
42.85	844,742399	AUX CLARKER	193023910002	arter .	Request. User anotymaus
140	STATE OF THE OWNER OWNE	10 A 46 A 47 A 46 A 46 A 46 A 46 A 46 A 46	S CORPORTING	FTP	Résource PASS 202111200 mp1 avects
1.50703	STRUM (ETTERNING	10.7.12.22	195.88.11.24	0.00	Request: Ust# Flercio

Zwracane są pary wpisów – jedna z nazwą użytkownika, druga – z hasłem.

6) Transmisja HTTPS

Na samym końcu spróbujemy podsłuchać transmisję szyfrowaną przy użyciu protokołu SSL. W tym celu włączamy filtr wyświetlania

Bie Edit Diese Go Capture Analyz	a Matistics Talaphony Isola Halp				
如此我我我 死 正因 X	日日 ヘキキの子:			15 X B	
Fytter: Jul	• 4	gression Clear Apply			
lin - Time	Source	Destination	Periocel	Into	
15200M 1007.155500	2011/22/22/	199.41.230.81	55L	COMPANY NO.	
132695 1607, 167661	193.41.230.81	10.7.12.22	TL SVL	Server sello	1
112698 1607, 168098	193.41.230.81	10.7.12.22	TCP	TCP segment of a reassembled PDU	
152699 1007.179515	193.41.210.81	10,7,12,22	TLSVI.	Certificate, Server mello Done	
152732 1607 224527	10,7,17,22	193.41.230.81	TL5V1	client key sycharge, change clipher spec. Entr	ypten Handshake Hes
152733 1607, 751394	193.41.230.81	10.7.12.22	R.SvL	Change Cipher Spec	
132734 1607.731715	193.41.230.81	10.7.12.22	TLSVI	Encrypted handshake Message	
132737 1607, 800120	191.41.210.81	10.7.12.22	TLSv1	Application Data	
152738 1607.800479	193.41.230.81	10.7.12.22	TCP	[TCP segment of a reassembled PDU]	
152739 1607,800483	193.41,230.81	10.7.12.22	TLSVE	Application Data	
132741 1608.022076	193.41.250.81	16.7.12.22	TCP	[TCP segment of a reassembled PDU]	
152742 1608.022459	193.41.230.81	10.7.12.22	TCP	TCP segment of a reassembled PDU	
152744 1608 022466	193.41.230.83	10.7.12.22	TCP	The segment of a reasonabled epul	
152746 1608,022869	193.41.230.81	10,7,12,22	TCP	[TCP segment of a reassembled PDU]	
152747 1606.022672	191.41.210.81	10.7.12.22	TCP	[TCP segment of a reassembled PDU]	
152748 1608.022877	193,41,230,81	10.7.12.22	TEP	[tc# segment of a reassembled PD0]	
**************************************		1000000000	-	and the second	
[stream index: 119]					
sequence number: 1 (re	nacive sequence number)				
Evert rednence unaper: 14	a (relative sequence num	ber)]			
Acknowledgement number: 1	(relative acc number)				
neader length: 20 bytes					
H Flags: UX18 (PSH, ACK)					
window st2e: 64240	ACCOUNT OF A DESCRIPTION				
H Criecksum: Oxfest@ [validat	fon disabled				
H [Sed/ACK analysis]					
secure socket Layer					
B TLSV1 Record Layer: Hands	hake Protocol: Client Hello				
500 00 0d 60 d5 c7 16 00 d5	ff f9 00 4e 08 00 45 00	AN ADDRESS OF THE REP.			
010 00 cf 03 2b 40 80 80 06	00 00 0a 07 0c 16 c1 29	Courses and the			1
020 em 51 e0 83 01 bb bd 93	10 68 02 15 46 05 50 18	-9N.P.			
040 01 4c 0f da 00 f2 af 2c	Se Sf bf 5d se c5 97 db	Children Without			
050 9a 67 12 6c 46 87 ab e6	83 cd 3c 78 04 a2 fc c3	.g. 1F \x			
060 le 00 00 46 c0 0a c0 14	00 88 00 87 00 39 00 38	A.F.F			
070 C0 UT C0 05 00 84 00 35 089 00 45 00 44 00 33 00 33	c0 07 c0 09 c0 11 c0 13 c0 0c c0 08 c0 02 c0 04				
And An 41 00 44 00 35 00 55	CO 00 CO 00 CO 02 CO 04				and a set
Realized WEINFORCED, WEINFORCED, NO.	1. F Residentes 35. Fight Phone in the second	down do 10		Photo	

Widzimy, że żadnych użytecznych danych niestety jawnie nie widać.